INFORMATION REGULATOR (SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information

FORM 15

ENFORCEMENT NOTICE IN TERMS OF SECTION 95 OF THE PROTECTION OF PERSONAL I NFORMATION ACT 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 12(2)(c)]

Reference number: **OIA-13-2023**

	DETAILS OF DATA SUBJECT
Name(s) & surname/ registered name of data subject/complainant/aggrieved party:	Information Regulator Own-Initiative Assessment in terms of section 89 of POPIA on First Rand Bank, known as First National Bank
Unique Identifier/ Identity Number	
Residential, postal or business address:	Woodmead North Office Park 54 Maxwell Drive Woodmead, Johannesburg 2191
Contact number(s):	010 023 5400
Fax number E-mail address:	[redacted]
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) & surname/ Registered name of responsible party:	First Rand Bank, known as First National Bank
Residential, postal or business address:	4 Merchant Place Corner Fredman Drive and Rivonia Road Sandton 2196
Contact number(s):	087-575-9404
Fax number/ E-mail address:	[redacted]

Be pleased to take notice that the Information Regulator (Regulator) after having conducted an own initiative assessment in terms of section 89 (1) of Protection of Personal Information Act 4 of 2012 (POPIA) decides that the responsible party has interfered with the protection of personal information of the data subjects as follows:

X	A breach of the conditions for the lawful processing of personal information.
	Non-compliance with the duty to notify security compromises (section 22 of the Protection of Personal Information Act 4 of 2013)
	Non-compliance with the duty of confidentiality (section 54 of the Protection of Personal Information Act 4 of 2013)
	Non-compliance with obligations for direct marketing by means of unsolicited electronic communications (section 69 of the Protection of Personal Information Act 4 of 2013)
	Non-compliance with obligations regarding the inclusion of personal information in directories (section 70 of Protection of Personal Information Act 4 of 2013)
	Non-compliance with obligations regarding automated decision making (section 71 of the Protection of Personal Information Act 4 of 2013)
	Non-compliance with obligations regarding personal information outside the Republic of South Africa (section 72 of the Protection of Personal Information Act 4 of 2013)
	Breach of the provision of a code of conduct issued in terms of section 60: Code of Conduct __of (Reference)

A. BREACH OF THE CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL INFORMATION

1. The responsible party has breached the conditions for the lawful processing of personal information as listed in the following sections of POPIA:

1.1. Condition 1 - Section 8 of POPIA

Responsible party to ensure conditions for lawful processing.

The responsible party must ensure that the conditions set out in this Chapter, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself.

1.1.1. After having considered all the submissions made by FNB in relation to its compliance with the eight conditions for the lawful processing of personal information, the Regulator determined that the deficiencies, failures and/or inadequacies in FNB's compliance framework results in FNB failing to comply with Condition 1 (section 8) as:

a. the Privacy Policy does not comply with the provisions of POPIA, in so far as it fails to adequately provide for all the rights afforded to data subjects in terms of section 5 of POPIA, including, in particular, the right contemplated in section 5(i) of POPIA;

b. the lawful justification for collection of personal information from newspapers is contrary to the provisions of section 12(2) of POPIA;

c. the Retention Schedule makes provision for the retention of records of personal information indefinitely without justification and such as contravenes section 14(1) of POPIA;

d. FNB relies on the incorrect exception for the further processing of personal information contrary to section 15(3) of POPIA; and

e. FNB failed to secure the confidentiality of personal information in its possession or under its control resulting in the compromise of data subject account information, in contravention of section 105 of POPIA.

1.2. Condition 2 - Section 9 - 12 of POPIA

Section 12- Collection directly from data subject

Personal information must be collected directly from data subject, except as otherwise provided for in subsection (2).

1.2.1. FNB states in paragraph 10 of its Customer Privacy Notice that it collects personal information directly from data subjects when engaging or interacting with FNB. This collection is done through various means, including but not limited to social media, emails, letters, telephone calls, and surveys.

1.2.2. FNB further states that it collects personal information from *public sources* such as newspapers, company registers, online search engines, deed registries, public posts on social media and public directories. This is mostly in line with its Anti Money Laundering (AML) Policies for purposes of enhanced due diligence on Politically Exposed Persons (PEP's) known as Prominent Influential Persons (PIP's).

1.2.3. Regarding the collection of personal information from newspapers, it is important to note that section 12(2)(a) of POPIA refers to a public record as opposed to a public source. The Regulator is of the firm view that this collection of personal information from newspapers does not fall under public record nor has the information contained in such newspaper deliberately been made public by the data subject. Therefore, this processing does not comply with the provision of section 12(2) of POPIA.

1.3. Condition 3: Purpose Specification and Retention and Restriction of records (section 13 and 14 of POPIA)

Retention and restriction of records (section 14 of POPIA)

POPIA provides that *records of personal information must not be retained*

any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed unless –

a) the retention of the record is required or authorised by law;
b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities;
c) retention is required by contract between the parties thereto; or
d) the data subject (competent person where the data subject is a child) has consented to retention.

1.3.1. Whilst the processing by FNB complies with the provisions of section 14(1)(a) and (b) of POPIA, the Regulator noted instances where FNB retains records indefinitely as reflected in its Retention Schedule such as:

- "*Cancelled or spoiled employees" tax certificates must be retained Indefinitely (page 11);*
- *Register identifying ownership of assets in terms of the Medical Schemes Act be retained indefinitely.*
- *Registers of securities and uncertificated securities be kept indefinitely (page 61) and others*".

1.3.2. The legal basis for such retention is not stated in the Retention Schedule and an explanation for same could not be provided by FNB. As such the retention of records of personal information for a period longer than required is in contravention of the provision of section 14(1) of POPIA.

1.4. Condition 4: Further Processing (section 15 of POPIA)

Further processing of personal information must be in accordance or compatible with the purpose for which it was collected in terms of section 13 of POPIA.

1.4.1. In paragraph 18 of its Customer Privacy Notice, FNB states that it will only share customers' personal information if the customer has consented to the processing, if it is necessary to conclude or perform under a contract the group has with the customer, if the law (FICA) requires it, or if it is necessary to protect or pursue the customer's, the groups, or a third party's legitimate interest.

1.4.2. The information that is stated in the aforementioned paragraphs specifically relating to further processing for the performance of a contract and the protection and pursuance of the data subjects, FNB's or a third parties' legitimate interest respectively are not exceptions for further processing referred to in section 15(3) of POPIA. Therefore, the processing does not comply with section 15(3) of POPIA in this instance.

1.5. Condition 7: Security Safeguards

Section 19 – Security measures on integrity and confidentiality of personal information

A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—

(a) loss of, damage to or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information.

1.5.1. On 21 February 2022, FNB confirmed a security compromise, in which the personal information of 88 data subjects was exposed to 696 unauthorised individuals. Aspects of this compromise were later confirmed when the Regulator received a complaint.

1.5.2. The unlawful access was as a result of some individual account holders being classified as employees. This resulted in them having access to the personal information of home loan applicants.

1.5.3. The type of information that was exposed to 696 unauthorised individuals included *inter-alia* names, identity numbers, contact details, physical address, income and salary information and account numbers.

1.5.4. This information was exposed on the FNB banking app where these unauthorised individuals had access to a list of names and ID numbers. When the list item with the name and ID number was clicked, all the personal information linked to the application would be exposed to the unauthorised individual.

1.5.5. Two previous instances of this exposure of personal information had been brought to the attention of FirstRand on separate occasions.

1.5.6. The first alert was through a customer referred to by FNB as *'Customer A'*, who alerted the bank that they were able to view in-progress loan applications of other customers on 30 March 2022.

1.5.7. The second alert was a customer referred to by FNB as *'Customer B'*, who on 3 May 2022 brought to the attention of the bank that they could view other users' in-progress home loan applications, however the issue was not resolved, as the complaint was acknowledged by FirstRand on 27 September 2022.

1.5.8. FNB did not address this vulnerability to the confidentiality of personal information even after two alerts by two parties who were mindful of the fact that they should not have been able to have access to such personal information.

1.5.9. It is plausible to assume that there may be a threat posed by other parties who viewed this personal information without alerting FirstRand of those actions afterwards.

1.5.10. The personal information that was exposed poses a threat of identity theft and circumventing (Know Your Customer) KYC verification at banks as well as putting the data subjects impacted in risk of sim swap scam, fraudulent activities, amongst a myriad of adverse effects.

1.5.11. The danger to the data subjects is compounded by the availability of compromised credit bureau data on the worldwide web. The risk that could adversely impact data subjects is that any information that is exposed, could be enriched using personal information from other breaches and enable opportunities for identity theft.

1.5.12. From the time that this issue was initially raised with FNB, up to the time the complaint was lodged to the Regulator, FNB had not addressed the vulnerability but resolved incidents that were reported without identifying them as unlawful access to personal information.

1.5.13. It is plausible to assume that there may be a threat posed by other parties who viewed this personal information without alerting FirstRand of those actions afterwards.

1.5.14. The personal information that was exposed poses a threat of identity theft and circumventing (Know Your Customer) KYC verification at banks as well as putting the data subjects impacted in risk of sim swap scam, fraudulent activities, amongst a myriad of adverse effects.

1.5.15. The danger to the data subjects is compounded by the availability of previously compromised credit bureau data available on the worldwide web. The risk that could adversely impact data subjects is that any information that is exposed could be enriched using information from other breaches and enable the opportunities for identity theft and fraud.

1.5.16. Due to this failure by FNB to correctly classify incidents and identify the compromises to personal information and handling them appropriately, FNB failed to secure the confidentiality of personal information in its possession by taking appropriate, reasonable technical and organisational measures to prevent unlawful access to personal information in accordance with section 19(1)(b) of POPIA.

1.6. **Section 105 – Dealing with an account number by a responsible party**

UNLAWFUL ACTS BY RESPONSIBLE PARTY IN CONNECTION WITH ACCOUNT NUMBER

1. *A responsible party who contravenes the provisions of section 8 insofar as those provisions relate to the processing of an account number of a data subject is, subject to subsections (2) and (3), guilty of an offence.*

2. *The contravention referred to in subsection (1) must—*

   a. *be of a serious or persistent nature; and*

   b. *likely cause substantial damage or distress to the data subject.*

3. *The responsible party must—*

   a. *have known or ought to have known that—*

      i. *there was a risk that the contravention would occur; or*

      ii. *such contravention would likely cause substantial damage or distress to the data subject; and*

   b. *have failed to take reasonable steps to prevent the contravention.*

4. *Whenever a responsible party is charged with an offence under subsection (1), it is a valid defence to such a charge to contend that he or she has taken all reasonable steps to comply with the provisions of section 8.*

5. *'Account number'', for purposes of this section and section 106, means any unique identifier that has been assigned—*

   a. *to one data subject only; or*

   b. *jointly to more than one data subject,*

   by a financial or other institution which enables the data subject, referred to in paragraph (a), to access his, her or its own funds or to access credit facilities or which enables a data subject, referred to in paragraph (b), to access joint funds or to access joint credit facilities.

1.6.1. **Section 105(2)(a), the interference with personal information was of a serious nature.**

a. The personal information of 88 data subjects including the contact information and account numbers of nine of those data subjects were accessed by 696 unauthorised individuals.

b. The personal information of these nine data subjects which could potentially have been accessed by six hundred and ninety-six individuals, could have resulted in multiple instances of unauthorised access to their personal information. Consequently, each unauthorised access represented a potential exposure of the affected data subjects' personal information to risks including, potential misuse, disclosure, or further compromise of their personal information.

c. The Regulator has had regard to the fact that there have been other security compromises where personal information had been unlawfully acquired and/or accessed, unrelated to the FNB security compromise such as those affecting credit bureaus. The existence of these security compromises increases the overall risk exposure and potential cumulative impact on the nine data subjects whose personal information was compromised. This raises concerns regarding the potential for further unauthorised access, disclosure or misuse of the affected personal information.

d. The interference was persistent. *Customer 'A'* first brought this interference to the attention of FNB in March. The unlawful access of that individual was removed, but the compromise to the personal information of data subjects was not reported to the Regulator.

e. There was an opportunity for an investigation by FNB which could have further revealed the gravity of the compromise.

f. *Customer 'B'* brought the same unlawful access to the attention of FNB, which was again resolved in respect of that one party without the security compromised being reported to the Regulator for action.

g. By the time a complaint was received by the Regulator in September, significant time had elapsed and even more time passed while internal investigations were conducted.

1.6.2. **Section 105(2)(b), The likelihood of substantial damage to the nine data subjects whose account numbers were accessed.**

a. The data subjects were susceptible to 696 ways to potentially impact them adversely. Though FNB did not cause the other previous compromises, the Regulator cannot discount the fact that the personal information that has been unlawfully accessed and/or acquired in other security compromises like the credit bureaus (Experian and Transunion) and may be merged or aggregated with other data to form complete profiles of data subjects.

b. This adds to the potential adverse impact to data subjects if this information would to be aggregated or merged with personal information that is already in the *wild* (open internet). This has the potential to circumvent the KYC checks if unauthorised persons are in possession of such sensitive information that is meant to be confidential.

1.6.3. **Section 105(3)(a)(i) – The responsible party should have been aware that the contravention would occur.**

a. As ventilated above, there were multiple opportunities for the responsible party to investigate and remedy the instances of interference with personal information, however, this was not done.

b. Over a period of months, FNB failed to detect that a contravention of section 19 was occurring due to attending to the "*incidents*" as isolated incidents. FNB was therefore unable to detect the vulnerability for what it was.

1.6.4. **Section 105(3)(a)(ii)**

a. FNB has an Access Management Policy in place that details how privileged access must be managed. This management of privileged access prevents unauthorised parties from accessing personal information of the data subjects in FNB's possession or under its control.

b. The fact that the configuration of the access measures was incorrect, meant that the harms that the responsible failed to address would now manifest.

1.6.5. **Section 105(3)(b)**

a. The repeated disclosures by other data subjects who found themselves with access, sought to give FNB an advantage in getting ahead of the compromise.

b. The reporting parties must have been concerned that their information may also be visible to some other parties, however, the ignorant manner in which a compromise to personal information reported to the responsible party was responded to, leaves a much to be desired as is reflective of the lackadaisical manner in which FNB handled these incidents.

c. This begs the question of how much longer the personal information would have be exposed, were it not for the Regulator's involvement and initiation of an assessment against FNB.

d. Against the above backdrop, FNB has committed an offence in terms of section 105(1) of POPIA in that it committed an unlawful act in relation to the account numbers of 88 data subjects by not complying with the provisions of section 19 of POPIA in relation thereto.

e. FNB knew or ought to have known that there was a risk that the contravention would occur and/or that such contravention would likely cause substantial damage or distress to data subjects and failed to take reasonable steps to prevent the contravention in terms of section 105(3) of POPIA.

1.7. Section 109(3) of POPIA

3. When determining an appropriate fine, the Regulator must consider the following factors:

a. the nature of the personal information involved;
b. the duration and extent of the contravention;
c. the number of data subjects affected or potentially affected by the contravention;

d. whether or not the contravention raises an issue of public importance;

e. the likelihood of substantial damage or distress, including injury to feelings or anxiety suffered by data subjects;

f. whether the responsible party or a third party could have prevented the contravention from occurring;

g. any failure to carry out a risk assessment or a failure to operate good policies, procedures and practices to protect personal information; and

h. whether the responsible party has previously committed an offence in terms of this Act.

a. the nature of the personal information involved;

The type of information that was exposed to 696 unauthorised individuals included names, surname, contact details, physical address, race, marital status and the account numbers of nine data subjects.

b. the duration and extent of the contravention;

i. A customer referred to by FNB as *'Customer A'*, first alerted the bank that they were able to view in-progress loan applications of other customers on 30 March 2022.

ii. The second alert was by a customer referred to by FNB as *'Customer B'*, who on 3 May 2022 brought to the attention of the bank that they could view other users' in-progress home loan applications. The issue was, however, not comprehensively attended to.

iii. Subsequent to the above incidents, a complainant lodged a complaint with the Regulator in relation to a similar set of facts on 27 September 2022.

iv. FNB did not address this vulnerability to the confidentiality of personal information even after the two alerts by the two customers who were mindful of the fact that they should not have been able to have access to such personal information.

v. This points to the persistent nature of this security compromise, where a failure in being able to identify interference with personal information left data subjects without confidentiality or integrity to their personal information.

c. the number of data subjects affected or potentially affected by the contravention;**

The personal information of 88 data subjects was exposed to the 696 unauthorised persons, with nine data subjects' account numbers being exposed.

d. whether or not the contravention raises an issue of public importance;

This compromise raises an issue of public importance because the potential exposure of personal information of 88 extends beyond the impact on the individual data subjects and implicates broader concerns

regarding the adequacy of information security measures and the protection of personal information.

The fact that there have also been other security compromises unrelated to the FNB compromise heightens these concerns by demonstrating the broader risks associated with the compromise of personal information.

This matter therefore has public interest implication in respect of the protection of personal information, information security, organisational accountability and maintaining public confidence in institutions entrusted with personal information.

e. the likelihood of substantial damage or distress, including injury to feelings or anxiety suffered by data subjects;

Although FNB submits that there was minimal risk of harm based on the mitigation measures implemented by it, the likelihood of distress and anxiety suffered by all FNB clients (those impacted and not impacted) should not be trivialized.

The potential for fraud, identity theft, and financial crimes arising from the exposure of this information is likely to cause substantial damage, distress and/or anxiety to affected data subjects.

f. whether the responsible party or a third party could have prevented the contravention from occurring;

The response to the above question is in the affirmative. *Customer "A"* first alerted the bank that they were able to view in-progress loan applications of other customers on 30 March 2022. At this stage, FNB should have noticed the breach and acted.

The second alert was a customer referred to by FNB as *'Customer B',* who on 3 May 2022 brought to the attention of the bank that they could view other users' in-progress home loan applications; however, the issue was not comprehensively dealt with.

The complaint lodged with the Regulator, which was acknowledged by FNB on 27 September 2022, presented a further opportunity for the FNB to take appropriate action. However, it failed to do so, continuing to treat the incidents as isolated occurrences rather than addressing them as part of a broader issue.

g. any failure to carry out a risk assessment or a failure to operate good policies, procedures and practices to protect personal information; and

This was a failure to operate good policies, procedure and practices to protect personal information as FNB failed to comply with section 19 of POPIA.

Further to this, FNB failed to adhere to its own policies on incident response and access management, thereby failing to secure the confidentiality of persona information in its control.

h. whether the responsible party has previously committed an offence in terms of this Act.

Not applicable

B. THE RESPONSIBLE PARTY IS HEREBY ORDERED TO:

Take the following specified steps:

1. In respect of the breach of Condition 1 of POPIA:

FNB is required to:

1.1. FNB must amend its Privacy Policy and/or Notice to :

a. make provision for section 5(i) of POPIA;
b. to state the lawful justification for collection of personal information in the newspapers as required by section 12 of POPIA and
c. revise the wording of paragraph 18 to distinguish between the lawful grounds for the initial collection of personal information and the specific exceptions permitting further processing under section 15(3) of POPIA.

2. In respect of the breach of Condition 2 of POPIA:

Section 12 – Collection directly from the data subject

FNB is required to:

a. Where personal information obtained from newspapers or other public sources does not meet the requirements of section 12(2)(a), FNB should assess and document whether another lawful justification under POPIA permits the collection. Where no applicable justification exists, FNB should refrain from collecting or further processing such information for the relevant purpose.

3. In respect of the breach of Condition 3 of POPIA:

Section 12 – Collection directly from the data subject

FNB is required to:

3.1. FNB must conduct a review of is governance framework in relation to retention of records and provide the Regulator with a detailed report. The report must further detail the steps that FNB will undertake to delete and/or destroy all information that:

a. It has retained longer than is necessary to achieve the purpose;

3.2. FNB must appoint a records management company who will destroy all documents that have been kept indefinitely with no legal basis and provide the Regulator with a copy of the destruction certificate;

3.3. Copies of the amended governance frameworks pertaining to retention of records must be amended to reflect the legal basis for all records of personal information retained by FNB.

4. In respect of the breach of Condition 4 of POPIA:

Section 15 – Further processing to be compatible with purpose of collection

FNB is required to:

4.1. Identify and assess the purposes for which customers' personal information is further processed or shared within the group and with third parties. For each activity, document the original purpose of collection, the intended further processing purpose and the applicable exception under section 15(3). Where no applicable exception exists, FNB should refrain from the further processing unless another lawful basis under POPIA permits it.

5. In respect of the breach of Condition 7 of POPIA

Section 19 – Security measures on integrity and confidentiality of personal information

FNB is required to:

5.1. FNB must ensure that the measures pertaining to the integrity of personal information documented are adequate to ensure that the personal information of data subjects in the possession of the responsible party is not subject to alteration or changes that may adversely impact the data subject;

5.2. FNB must ensure that the identified and documented security safeguards are implemented, verified and tested to ensure that they are effective and adequate to protect the confidentiality and integrity of personal information under the responsibility of FirstRand;

5.3. FNB must ensure that all vulnerabilities pertaining to the integrity and confidentiality of personal information in its possession its under its control are assessed and if they pose serious threat to one or more data subjects, are addressed and eliminated if possible;

5.4. FNB must review and strengthen role-based access control measures to ensure that only individuals who have responsibility in a specific domain has access to processing of that personal information.

5.5. FNB must ensure that employees are trained in identifying information security incidents and report them as per the functional standard.

6. In respect of the breach of section 105 of POPIA

FNB is required to:

6.1. FNB be liable to a fine for the offence of exposing the account numbers (as defined by section 105(5)) of nine data subjects in terms of section 105(1) of POPIA.

C. TIME PERIODS

First National Bank must provide the Regulator within **90** days of receipt of this report, a full report containing supporting documentary evidence on the implementation of all the above recommendations.

D. RIGHT OF APPEAL

The responsible party may appeal against this Enforcement Notice within 30 days of the date of receipt of this Enforcement Notice as provided for in section 97(1) of POPIA.

E. CONSEQUENCES FOR NON-COMPLIANCE WITH AN ENFORCEMENT NOTICE

Please note that a responsible party which fails to comply with this Enforcement Notice is guilty of an offence and liable upon conviction to fine or to imprisonment for a period not exceeding 10 years or to both such a fine and such imprisonment.

Dated at **Johannesburg** on **21 October 2026.**

[redacted].

Adv. Pansy Tlakula
Chairperson of the Information Regulator